Ebook

NIS 2 : quels impacts pour les RSSI ?

Guide de survie pour vous conformer à cette directive

SIGMA
NUMÉRIQUE À IMPACT

_Edito

« Ode à la solitude du RSSI européen »

En sa qualité de chef d'orchestre de la sécurité de l'information, le RSSI européen peut se sentir bien seul.

Rempart contre la cyber-insécurité, il coordonne inlassablement ses efforts sur de nombreux fronts pour s'assurer d'une stratégie cyber sans fausse note.

Mais alors que la cyber-guerre prend une dimension géopolitique et que **les cyber-risques constituent désormais le principal risque commercial pour les entreprises** (Allianz Risk Barometer 2024), peut-on raisonnablement le laisser seul dans les tranchées ?

NIS 2 débarque en Europe comme une leçon de solfège : pour composer notre « ode à la joie » en termes de cybersécurité européenne, il faudra désormais composer « de concert » notre mélodie des bonnes pratiques de sécurité.

_Quand l'Europe donne le LA de la Cybersécurité

NIS 2, qu'est-ce que c'est ?

La directive NIS 2 est un **texte législatif de l'Union européenne** sur la cybersécurité. Le texte est basé sur la gestion des risques. Il remplace et complète la directive NIS première du nom (Network and Information Security), adoptée en juillet 2016. La directive NIS 2 **dresse une liste de mesures a minima devant être prises par toutes les entités**.

NIS 2 en 10 thématiques

1. Les politiques relatives à l'analyse des risques et à la sécurité des systèmes d'information
2. La gestion et le traitement des incidents
3. La continuité des activités, comme la gestion des sauvegardes et la reprise des activités
4. La sécurité de la chaîne d'approvisionnement
5. La sécurité de l'acquisition, du développement et de la maintenance des réseaux et des systèmes d'information
6. L'évaluation des mesures de gestion des risques liés à la cybersécurité
7. La formation à la cybersécurité et cyber hygiène
8. Les politiques et procédures relatives à l'utilisation de la cryptographie et, le cas échéant, du chiffrement
9. La sécurité des ressources humaines, des politiques de contrôle d'accès et la gestion des actifs
10. L'utilisation de solutions d'authentification à plusieurs facteurs

Directive (UE) 2022/2555 du parlement européen et du conseil du 14 décembre 2022

« La cybersécurité : avant c'est trop cher, après c'est trop tard »

Sylvain B.P. RSSI Blog Mediapart

Source : Webinar Sigma - Directive NIS2 et cyber : 5 étapes vers la conformité

Pourquoi encore une directive ?

- Faire coopérer les **Etats membres de l'UE** pour améliorer la cybersécurité.
- Couvrir un plus grand nombre d'entités et de secteurs pour une **protection plus complète**.
- Mettre en place un **système unifié** pour signaler les incidents de cybersécurité et gérer les cybercrises.
- Renforcer la sécurité de la **chaîne d'approvisionnement** et s'attaquer aux nouvelles **menaces cybernétiques**.

Mais qui est concerné par cette directive ?

ENTITÉS ESSENTIELLES
Secteurs HAUTEMENT CRITIQUES

ÉNERGIE

- ÉLECTRICITÉ
- GAZ
- PÉTROLE
- HYDROGÈNE
- RÉSEAUX CHALEUR & FROID

TRANSPORTS

- AÉRIENS
- FERROVIAIRES
- PAR EAU
- ROUTIERS

- EAU POTABLE
- EAUX USÉES
- ADMINISTRATION PUBLIQUE
- INFRASTRUCTURE NUMÉRIQUE
- BANQUES
- INFRASTRUCTURES DES MARCHÉS FINANCIERS
- GESTION DES SERVICES TIC
- ESPACE
- SANTÉ

> 250

CA > 50M€ ou BA > 43M€

ENTITÉS IMPORTANTES
Autres secteurs CRITIQUES

- SERVICES POSTAUX & EXPEDITION
- GESTION DES DÉCHETS
- PRODUITS CHIMIQUES
- FOURNISSEURS NUMÉRIQUES
- DENRÉES ALIMENTAIRES
- RECHERCHES

FABRICATION

- DISPOSITIFS MÉDICAUX & DE DIAGNOSTIC IN-VITRO
- INFORMATIQUES, ÉLECTRONIQUES & OPTIQUES
- ÉQUIPEMENTS ÉLECTRIQUES
- MACHINES N.C.A
- VÉHICULES AUTOMOBILES ET REMORQUES
- MATÉRIELS DE TRANSPORTS

> 250

10 > CA > 50M€ ou 10 > BA > 43M€

https://blog.interdata.fr/article-la-directive-network-and-information-security

NIS 2 : régulation et sanctions

ENTITÉS ESSENTIELLES	ENTITÉS IMPORTANTES
Déclarations d'incidents	
Notification sous 24h des **incidents de sécurité importants** à l'ANSSI Notification sous 72h d'une **mise à jour avec évaluation initiale** (gravité, impact, IoC) A la demande de l'ANSSI, un **rapport intermédiaire** sur les mises à jour pertinentes de la situation Un **rapport final** sous 1 mois (description détaillée, cause racine, mesures d'atténuation)	
Régulation	
Régulation dite «ex-ante» ***(contrôle à discrétion de l'ANSSI)***	Régulation dite «ex-post» ***(contrôle en cas de connaissance d'une non-conformité)***
Sanctions	
10 millions d'euros ou **2% du chiffre d'affaires annuel mondial**	7 millions d'euros ou **1,4% du chiffre d'affaires annuel mondial**

Renforcer la cybersécurité des services essentiels au bon fonctionnement de notre société, c'est l'ambition de la directive européenne NIS 2 (Network Information Security) fixée à octobre 2024, **son application concerne 18 secteurs du privé et du public**.

Pourtant, **seules 14 % des entreprises affirment s'être déjà mises en conformité sur les objectifs de la directive NIS 2** (selon une étude publiée par Zscaler*).

**Source : NIS 2 & Beyond : Risk, Reward & Regulation Readiness, l'étude recense les retours de plus de 875 responsables informatiques sur six marchés européens.*

Appliquer les bonnes pratiques de cybersécurité est une assurance pour rester une organisation **saine et performante** en toute circonstance dans les années à venir (qui verront arriver de nouvelles menaces cybernétiques et leur cortège de législation pour les contrer) et nous sommes là pour vous accompagner pas à pas en fonction de votre **situation initiale**.

_Votre trajectoire cyber : les bonnes pratiques pour tous et par tous

0 = Evaluation du risque

- **Cartographier** les services critiques et les écosystèmes (infras, applications, data inhérentes)
- **Recenser** les parties prenantes (internes et externes)
- **Auditer** son SI, son organisation pour poser un diagnostic de ses vulnérabilités et expositions aux risques (varier les audits de sécurité et effectuer des pentests réguliers)

1 = Gouvernance

- **S'inscrire** auprès de l'ANSSI pour être conseillé et accompagné
- **Impliquer** son management pour intégrer la cybermenace comme risque stratégique
- **Adapter** les politiques de sécurité et les partager largement aux directeurs opérationnels

2 = Ressources et sensibilisation

- **Adapter** son dispositif humain en intégrant les compétences et l'expertise de votre secteur d'activité et vos engagements de services
- **Capitaliser** sur les bonnes pratiques pour rentabiliser les actions
- **Faire collaborer** Infrastructures et Sécurité pour la prévention et détection – réponse à l'incident
- **Mettre en place** des workflows impliquant toute l'organisation
- **Former** les équipes IT aux méthodes et processus de cybersécurité et gestion de crise
- **Sensibiliser** les collaborateurs aux bonnes pratiques pour acculturer et faire adopter les bons réflexes (Campagnes de phishing)

Découvrez nos accompagnements Cybersécurité : en savoir plus

3 = Gestion des accès

- **Gérer** les accès physiques
- **Mettre en place** une authentification forte (MFA)
- **Administrer** finement les identités et les accès
- **Gérer** les interconnexions des SI

4 = Durcissement des configurations

- **Opter** pour une stratégie de durcissement et d'authentification : abastion, réseaux et gateway, web application firewall...
- **Cloisonner** les systèmes et créer bastions et air gap
- **Gérer** la granularité des configurations administrateur des SI
- **Instaurer** des politiques fiables de revue des applications

5 = Gestion des communications

- **Chiffrer** les communications internes
- **Filtrer** les communications inter-systèmes

6 = Gestion des alertes

- **Mettre en place** une solution de réception des alertes ainsi qu'une solution de journalisation
- **Multiplier** les exercices de Cybercrise et impliquer l'ensemble de l'écosystème

7 = Résilience

- **Mettre en place** et **tester** régulièrement les plans de Reprise d'Activité (PRA) et Plan de continuité d'activité (PCA)
- **Interroger** et tester la politique de sauvegarde et veiller à respecter la règle des 3 – 2 -1 -1 (Chiffrement et immuabilité + indépendance des composants de production)
- **Mesurer** sa capacité à travailler en mode dégradé : papier et crayon !

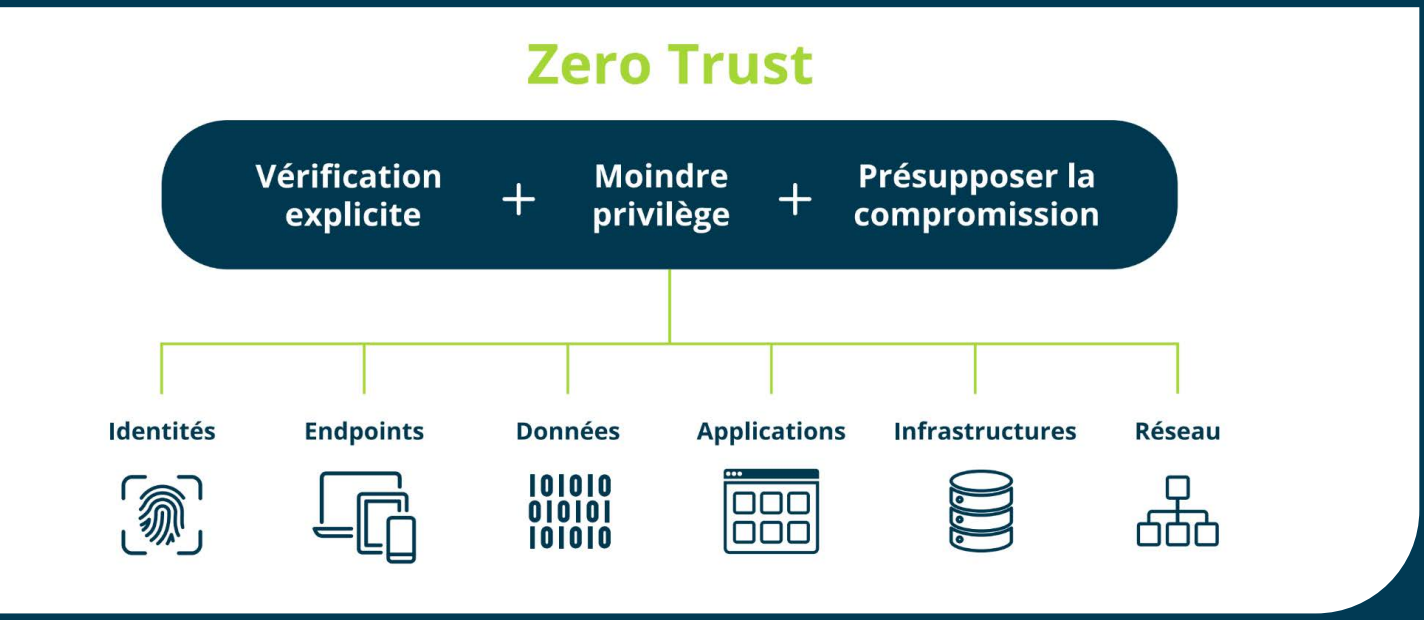
Votre conformité NIS 2 = Une pierre 3 coups

Avec Sigma, associez cybersécurité, durabilité et optimisation des coûts

La gestion du risque selon Sigma

Chez Sigma, nous travaillons sur des méthodes de pointe pour soulager les équipes IT et OT dans leur mise en conformité, et de façon plus générale, dans leurs tâches quotidiennes et dans la gestion du changement.

- Présupposer la compromission de ses actifs est une première étape indispensable pour **s'inscrire durablement dans le changement et prioriser ses investissements.**
- **L'expertise plurielle de Sigma** (infogérance, IT, cybersécurité et enjeux métier) permet la mise en place de **scénarios de risques personnalisés** en fonction de vos besoins et la prescription des solutions les plus adaptées.
- Sigma se distingue notamment par son **approche complète du Zero Trust** du conseil en mesure organisationnelle pour renforcer les niveaux d'authentification et des pratiques d'administration, de détection et de réponse aux incidents via des solutions technologiques telles que EDR, XDR, SIEM, CASB et SASE, couvrant ainsi tous les aspects des six piliers du modèle.



- **Une équipe SOC (Security Operations Center) disponible et basée en France en 24/7/365**

- Avec la **sécurisation Move To Cloud,** vous tirerez profit de tous les avantages du cloud, sans prendre de risque en termes de fiabilité et protection des données personnelles. Bénéficier des solutions de **sécurité opérationnelle « New Gen » basées sur le cloud et l'IA**

- **Un accompagnement complet et modulable** pour votre mise en conformité alliant une sensibilisation à la sécurité informatique, l'anticipation des menaces avec la mise en place et le suivi de stratégies cybersécurité sur-mesure, le déploiement de plans de remédiation, de continuité (PCA) et de reprise d'activité (PRA) adaptés à vos enjeux

- Un accompagnement continu pour garantir une **compréhension approfondie et une mise en œuvre efficace de cette approche durable de la sécurisation des actifs**

- Des **parcours ludiques de sensibilisation** autour des usages des collaborateurs, pour adapter leurs pratiques et les ancrer dans une démarche volontaire et continue, à l'aide notamment de contenus didactiques, récurrents, non-anxiogènes et des exercices de mises en situations réelles

Un seul objectif : ne pas laisser les RSSI seuls et désemparés face à l'ampleur de la tâche de la mise en conformité cyber.

À PROPOS DE SIGMA

Sigma est une entreprise du numérique, spécialisée dans l'édition et l'intégration de logiciels et de solutions sur mesure, l'externalisation de systèmes d'information et les solutions cloud, la cybersécurité et la valorisation des données.

Notre raison d'être :
« Apporter à notre écosystème des solutions numériques qui contribuent à un futur désirable dans lequel chacun et chacune trouve sa place ».

SiGMA
NUMÉRIQUE À IMPACT

La Gesvrine - 8 rue Newton
La Chapelle-sur-Erdre
Tel. : +33 (0)2 40 37 14 00
https://www.sigma.fr
@groupesigma

SIGMA : créer plus de performance par le numérique à impact.

Nous servons votre performance économique, sociale et environnementale en révélant les potentiels de vos écosystèmes informatiques. Nous militons pour un numérique à impact permettant de construire, avec vous, des services numériques utiles aux femmes et aux hommes, dans le respect du vivant.
Notre trajectoire : innover pour vous apporter des solutions éco-conçues.
D'ici 2026 : -40% de nos émissions GES et +50 % de nos solutions éco-conçues.

Nantes
Paris
Lyon
Toulouse
Strasbourg

700 collaborateurs sur 5 implantations nationales

10 partenaires technologiques majeurs

2200 clients

75 M€ de CA

5 piliers numériques majeurs

- Édition et intégration
- Solutions sur-mesure
- Data valorisation
- Infogérance et Cloud services
- Cybersécurité